

## **SFA Security Policy Table of Contents**

<b>SFA Security Policy .....</b>	<b>2</b>
<b>1.0 Introduction .....</b>	<b>2</b>
<b>2.0 Management Controls .....</b>	<b>2</b>
<b>2.1 Risk Management .....</b>	<b>2</b>
<b>2.2 Security Control Reviews .....</b>	<b>2</b>
<b>2.3 System Security Plan .....</b>	<b>2</b>
<b>2.4 Rules of Behavior .....</b>	<b>2</b>
<b>2.5 Solution Life Cycle .....</b>	<b>2</b>
<b>2.6 Certification and Accreditation .....</b>	<b>3</b>
<b>2.7 Security Awareness and Training.....</b>	<b>3</b>
<b>2.8 System Interconnections .....</b>	<b>3</b>
<b>3.0 Operational Controls .....</b>	<b>3</b>
<b>3.1 Personnel Security .....</b>	<b>3</b>
<b>3.2 Physical and Environmental Protection.....</b>	<b>3</b>
<b>3.3 Production, Input/Output Controls .....</b>	<b>4</b>
<b>3.4 Contingency Planning/Disaster Recovery Plan.....</b>	<b>4</b>
<b>3.5 Data Integrity.....</b>	<b>4</b>
<b>3.6 Documentation .....</b>	<b>4</b>
<b>3.7 Configuration Management .....</b>	<b>4</b>
<b>3.8 Incident Response Capability.....</b>	<b>4</b>
<b>4.0 Technical Controls .....</b>	<b>5</b>
<b>4.1 Identification and Authentication.....</b>	<b>5</b>
<b>4.2 Logical Access Controls .....</b>	<b>5</b>
<b>4.3 Audit Trails .....</b>	<b>5</b>

# **SFA Security Policy**

## **1.0 Introduction**

- 1.1 Purpose**
- 1.2 Scope**
- 1.3 SFA Security Fundamentals**
- 1.4 Compliance**
- 1.5 Exceptions**
- 1.6 Applicability**
- 1.7 Policy Administration**
- 1.8 References**
- 1.9 Strategies**
- 1.10 Security Organization**
- 1.11 Roles and Responsibilities**
- 1.12 Document Structure**
  - 1.12.1 Management Controls**
  - 1.12.2 Operational Controls**
  - 1.12.3 Technical Controls**

## **2.0 Management Controls**

- 2.1 Risk Management**
  - 2.1.1 Risk Assessment**
    - 2.1.1.1 Sensitivity Analysis
  - 2.1.2 Risk Mitigation**
    - 2.1.2.1 Business Impact Analysis
    - 2.1.2.2 Consequence Assessment
    - 2.1.2.3 Countermeasure Analysis
- 2.2 Security Control Reviews**
  - 2.2.1 A-130**
  - 2.2.2 NIST Self-Assessment**
  - 2.2.3 Corrective Action Plans**
- 2.3 System Security Plan**
  - 2.3.1 General Policy**
  - 2.3.2 Configuration Management**
  - 2.3.3 Document Control**
  - 2.3.4 Enterprise Policy**
- 2.4 Rules of Behavior**
  - 2.4.1 General Policy**
  - 2.4.2 Specific Policy for Users**
- 2.5 Solution Life Cycle**
  - 2.5.1 General**
  - 2.5.2 Vision**
    - 2.5.2.1 Business Case
  - 2.5.3 Definition**
    - 2.5.3.1 Sensitivity Assessment

2.5.3.2 Security Requirements

**2.5.4 Construction**

2.5.4.1 RFP Requirements

2.5.4.2 Testing Procedures

2.5.4.3 Security Requirements

2.5.4.4 Risk

**2.5.5 Deployment**

2.5.5.1 Certification and Accreditation

2.5.5.2 Configuration Management

2.5.5.3 Security Awareness

2.5.5.4 Post-acceptance Security Controls

2.5.5.5 Design Reviews and System Tests

**2.5.6 Support**

2.5.6.1 Audits and Reviews

2.5.6.2 Security Plan

2.5.6.3 Operational Assurance

2.5.6.4 Security Operations

**2.5.7 Retirement**

2.5.7.1 Information Disposal

2.5.7.2 Information Archival

**2.6 Certification and Accreditation**

**2.7 Security Awareness and Training**

**2.7.1 Training**

**2.7.2 Refresher Training**

**2.7.3 Awareness**

**2.7.4 Contractor**

**2.8 System Interconnections**

**3.0 Operational Controls**

**3.1 Personnel Security**

3.1.1 Position Sensitivity Level

3.1.2 Background Screening

3.1.3 Separation of Duties

3.1.4 Least Privilege

**3.2 Physical and Environmental Protection**

**3.2.1 Supporting Utility Security**

3.2.1.1 Air Conditioning

3.2.1.2 Water

3.2.1.3 Power

**3.2.2 Fire Control**

**3.2.3 Facilities**

3.2.3.1 Visitors

3.2.3.2 Access

3.2.3.3 Static Entry Codes

3.2.3.4 Suspicious Activities

**3.2.4 Data Intercept**

- 3.2.5 Media Labeling and Logging**
- 3.3 Production, Input/Output Controls**
  - 3.3.1 Electronic Media Sanitation**
  - 3.3.2 User Support**
  - 3.3.3 Hardcopy Destruction**
  - 3.3.4 Storage**
  - 3.3.5 Labeling**
  - 3.3.6 Access**
  - 3.3.7 Logging**
- 3.4 Contingency Planning/Disaster Recovery Plan**
  - 3.4.1 General Plans**
    - 3.4.1.1 Contingency Plan**
    - 3.4.1.2 Disaster Recovery Plan**
    - 3.4.1.3 Backup Plan**
    - 3.4.1.4 Emergency Plan**
  - 3.4.2 Testing**
    - 3.4.2.1 Alternate Processing Site**
- 3.5 Data Integrity**
  - 3.5.1 Virus Detection and Elimination**
  - 3.5.2 Reconciliation**
  - 3.5.3 Verification**
  - 3.5.4 Message Authentication**
  - 3.5.5 Performance Measurements**
  - 3.5.6 Intrusion Detection**
  - 3.5.7 Penetration Testing**
- 3.6 Documentation**
- 3.7 Configuration Management**
  - 3.7.1 General**
  - 3.7.2 Configuration Control Board**
    - 3.7.2.1 Change Management**
      - 3.7.2.1.1 Documentation**
      - 3.7.2.1.2 Testing**
      - 3.7.2.1.3 Approval**
      - 3.7.2.1.4 Emergency Changes**
  - 3.7.3 Procedures and Guidance**
    - 3.7.3.1 Maintenance and Repair**
    - 3.7.3.2 Illegal Software**
    - 3.7.3.3 Application Licensing**
- 3.8 Incident Response Capability**
  - 3.8.1 General**
  - 3.8.2 Preventative Measures**
  - 3.8.3 Incident Identification and Resolution**
    - 3.8.3.1 Incident Identification**
    - 3.8.3.2 Post Incident**
  - 3.8.4 Information Sharing**

## **4.0 Technical Controls**

- 4.1 Identification and Authentication**
  - 4.1.1 General Policy**
  - 4.1.2 Identification Accountability**
  - 4.1.3 Host Based Identification**
  - 4.1.4 Biometrics**
  - 4.1.5 Public Key Infrastructure**
  - 4.1.6 Passwords**
    - 4.1.6.1 Frequency of Change
    - 4.1.6.2 Format
      - 4.1.6.2.1 Compliance*
    - 4.1.6.3 Scripts with Passwords
  - 4.1.7 Bypassing Controls**
  - 4.1.8 Access Control Lists**
- 4.2 Logical Access Controls**
  - 4.2.1 General**
  - 4.2.2 Application**
  - 4.2.3 Files**
  - 4.2.4 Delegate Permission**
  - 4.2.5 Desktop**
  - 4.2.6 Firewall and Proxy**
  - 4.2.7 Encryption**
  - 4.2.8 Network**
  - 4.2.9 System Interconnection**
  - 4.2.10 Communication Security**
  - 4.2.11 Fraud Waste and Abuse**
  - 4.2.12 Web Policy**
    - 4.2.12.1 Web Site Privacy Policy
  - 4.2.13 Warning Banners**
  - 4.2.14 Remote Access**
- 4.3 Audit Trails**
  - 4.3.1 Review**
  - 4.3.2 Content**
  - 4.3.3 Access Control**
  - 4.3.4 Keystroke Monitoring**
  - 4.3.5 Separation of Duties**